The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

04/29/2013

SUBJECT:

Vulnerability in Ektron's Enterprise Web Content Management Solution Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Ektron's Enterprise Web Content Management Solution that can lead to remote code execution. Ektron's Enterprise Web Content Management Solution is used to create, deploy and manage enterprise-scale, personalized websites. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the content management solution. Depending on the privileges associated with the application, an attacker could execute arbitrary code in the context of the application, and bypass security restrictions.

It should be noted that this vulnerability is being actively exploited by attackers to compromise servers and exfiltrate data from the state and local government systems.

SYSTEMS AFFECTED:

- Versions prior to Ektron CMS 8.02 Service Pack 5 are vulnerable.

RISK:

Government:

- Small government entities: **High**
- Large and medium government entities**: High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

DESCRIPTION:

A vulnerability has been discovered in Ektron's Enterprise Web Content Management Solution that can lead to remote code execution. The vulnerability exists due to the insecure usage of XslCompiledTransform, an XSLT controlled by the user. In order to exploit this vulnerability, an attacker must create a specially crafted post request and send it to the vulnerable page located at "WorkArea/ContentDesigner/ekajaxtransform.aspx".

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the content management solution. Depending on the privileges associated with the application, an attacker could execute arbitrary code in the context of the application, and bypass security restrictions. In addition, failed attacks may cause denial-of-service conditions.

It should be noted that this vulnerability is being actively exploited by attackers to compromise servers and exfiltrate data from the state and local government systems.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Ektron immediately after appropriate testing.
- Limit access to the Ektron CMS from public Internet

REFERENCES:

Microsoft Technet:

http://technet.microsoft.com/en-us/security/msvr/msvr12-016#section6

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5357

SecurityFocus:

http://www.securityfocus.com/bid/56816